ABSTRACT OF THE DISCLOSURE

In a public key cryptosystem for utilization of private keys to encrypt or decrypt items transmitted over a network which is not secure, the private keys of users, as encrypted with a symmetric algorithm by using individual user identifying keys determined by hashing the users' respective passphrases or biometric information (fingerprint, voice print, retina scan, or face scan), are stored at the server end along with the users' respective public keys, indexed or addressable by user ID, and are sent to the user equipment only when needed. Further, after use, the private key and user identifying key are not retained at the user equipment. The server uses an ID of a user transmitted to it from user equipment to read the stored encrypted private key and the public key of the user. The encrypted private key is then transmitted via the network to the user equipment along with a document to be approved by the user (in the case where the private key is used for digital signature) and, locally, at the user equipment the received encrypted private key is decrypted using a key determined at the user equipment by hashing either the user's passphrase, which is entered by the user, or the user's biometric information which is obtained by measurement or scanning the user. The received document is modified or merely reviewed, and a digital signature signifying the user's approval thereof, is formed as a hash of the approved document encrypted using the user's private key. The digital signature and document are transmitted to the server, where verification takes place.